Deutscher Bundestag **Drucksache 17/8161**

17. Wahlperiode 14. 12. 2011

Antrag

der Abgeordneten Dr. Konstantin von Notz, Nicole Maisch, Tabea Rößner, Volker Beck (Köln), Ingrid Hönlinger, Memet Kilic, Jerzy Montag, Claudia Roth (Augsburg), Wolfgang Wieland, Josef Philip Winkler und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Grundrechte schützen – Datenschutz und Verbraucherschutz in sozialen Netzwerken stärken

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Soziale Netzwerke verzeichnen weiter hohe Zuwächse hinsichtlich der Anzahl der Nutzerinnen und Nutzer. Allein der Marktführer Facebook verfügt bereits über 23 Millionen deutsche Mitglieder. Die Angebote der VZ-Gruppe werden von 17 Millionen Personen genutzt. Die Anzahl der durch soziale Netzwerke bereitgestellten Angebote nimmt stetig zu. Kostenfreie Möglichkeiten der Informationsverwaltung und der Selbstpräsentation, erleichterte Möglichkeiten der Kontaktaufnahme, leicht zugängliche Informationen über Dritte und unterschiedliche Kommunikationsmöglichkeiten locken neben Privatpersonen auch Unternehmen sowie die unterschiedlichsten Berufsgruppen in die sozialen Netzwerke. Durch die Integration von redaktionellen Angeboten, Spielen und E-Commerce-Marktplätzen entwickeln sich einige soziale Netzwerke zu umfassenden Netzen im Netz, die auch auf anderen Webseiten durch Interaktionsmöglichkeiten präsent sind (z. B. durch sog. Social Plugins).

Der Deutsche Bundestag begrüßt die Angebote sozialer Netzwerke, insbesondere die mit ihnen verbundenen, erleichterten Möglichkeiten der Verbreitung von und des Zugangs zu Informationen, die Bildung von interessengeleiteten Gruppen, die erleichterte Kontaktaufnahme zwischen Menschen und unterschiedlichsten Institutionen sowie die vereinfachten interaktiven, weltweiten Kommunikationsmöglichkeiten. Sie sind zentrales Element eines Internets, das die rein rezeptive Aufnahme von Informationen ergänzt und Interaktivität in den Vordergrund stellt. Die Nutzung sozialer Netzwerke selbst kann in mehrfacher Hinsicht als Grundrechtsausübung gelten und die wachsende Zahl der Mitglieder belegt ihre derzeitige hohe gesellschaftliche Relevanz.

Der Deutsche Bundestag betont, dass es sich bei den Betreibern sozialer Netzwerke dem Geschäftsmodell nach um Werbe- und Marktforschungsunternehmen handelt, wobei die marktführenden Unternehmen ihren Firmensitz in den USA haben und damit deren Datenverarbeitungen in Drittländern außerhalb der EU erfolgen, während sich die Angebote erkennbar an den bundesdeutschen Markt richten. Daraus folgende Unklarheiten hinsichtlich der Anwendbarkeit und der Durchsetzbarkeit bundesdeutscher Datenschutzbestimmungen dürfen nicht zu Lasten der Verbraucherinnen und Verbraucher gehen.

Die Mehrzahl der bereitgestellten Angebote wird kostenlos angeboten. Einnahmen werden deshalb regelmäßig über das möglichst zielgerichtete Bewerben der Angebote von Drittunternehmen erreicht. Voraussetzung dafür sind umfängliche Informationen über die individuellen Nutzerinnen und Nutzer der Netzwerke. Diese Daten werden durch Auswertung sowohl der aktiv von den Nutzerinnen und Nutzern eingestellten Daten als auch durch Auswertung des Gesamtverhaltens auf der Plattform und im Internet mit Hilfe von Techniken der Beobachtung und der Analyse von Verkehrsdaten (Click-Stream-Analyse; Cookies, Zählpixel, etc.) vorgenommen. Dabei werden bei einzelnen Anwendungen (Beispiel Social Plugins) offenbar auch die Daten von Nichtmitgliedern erfasst und gespeichert. Daten von Nichtmitgliedern gelangen ohne deren Wissen auch durch die aktive Nutzung bestimmter Angebote der Netzwerke durch Freunde und Bekannte (z. B. durch Hochladen von Adressbüchern, durch das sog. Tagging von Bildern) in den Datenbestand von sozialen Netzwerken. Bei sozialen Netzwerken muss deshalb zwischen der Ebene des Verhältnisses von Mitgliedern untereinander und der Ebene des Verhältnisses der Mitglieder und Nichtmitglieder zum jeweiligen Betreiber unterschieden werden, wobei datenschutzrechtliche Fragen auf allen Ebenen aufgeworfen werden.

Der Deutsche Bundestag zeigt sich besorgt über den Umgang mit persönlichen Daten und Informationen, die durch soziale Netzwerke im Internet allgemein zugänglich werden und oftmals besonders sensitiv sind. Soziale Netzwerke leben davon, dass ihre Mitglieder sich aktiv beteiligen und viele Einzelheiten über sich offenbaren. Dabei wird für die Nutzer oftmals der Eindruck weitgehender individueller Kontrolle über diese Informationen erweckt, während zentrale Teile der vorgenommenen Datenverarbeitungen nur den Betreibern bekannt sind. Gänzlich intransparent bleiben auch die vorgenommenen Datenverarbeitungen von integrierten Drittanbietern, die auf den Plattformen Zusatzprogramme wie Spiele oder die Anbindung an andere Webanwendungen anbieten. Forschungen belegen, dass der subjektive Eindruck individueller Kontrolle in deutlichem Widerspruch zur objektiv fehlenden Kontrolle über Daten und Informationen im Kontext des Internets steht. Zwar wächst etwa unter minderjährigen Nutzerinnen und Nutzern das Bewusstsein für die mit der Kommunikation in sozialen Netzwerken verbundenen Risiken. Selbstbestimmte Entscheidungen sind jedoch ob der hohen Popularität unter Jugendlichen auch bei verbesserter Medienkompetenz nicht immer möglich. Die wechselnden Nutzungsbedingungen der Anbieter sozialer Netzwerke erschweren häufig ein einfaches Verständnis und den Zugang zu datenschutzkonformen Grundeinstellungen. Möglichkeiten der Umgehung zugangsbehindernder Einstellungen durch Dritte (sog. Privatsphäreeinstellungen) und gravierende Datensicherheitsprobleme vermindern eine individuelle Kontrolle und schaffen Missbrauchsmöglichkeiten. Angesichts der zumeist umfänglichen Auswertung der Daten mit Hilfe komplexer Data-Mining-Verfahren durch die Plattformbetreiber können zudem umfängliche Verhaltens- und Persönlichkeitsprofile entstehen. Die Art und Weise der Erstellung sowie der Verwendung dieser Profile, zumeist für Werbezwecke, bleibt für die Nutzerinnen und Nutzer, aber auch für die zuständigen Aufsichtsbehörden weitgehend intransparent. Damit entstehen auch Risiken der Manipulierbarkeit, die in deutlichem Widerspruch zum Leitbild informierter Verbraucherinnen und Verbraucher stehen. Schließlich zeigen zunehmend Sicherheitsbehörden, aber auch Privatunternehmen, ein erhebliches Interesse an der Recherche zu Einzelpersonen und ihren Verbindungen zu weiteren Personen in sozialen Netzwerken. Über 50 Prozent der Personalverantwortlichen geben etwa an, in sozialen Netzwerken Recherchen zu Beschäftigten und Bewerberinnen und Bewerbern durchzuführen und stellen damit bislang geltende Grenzen des Beschäftigtendatenschutzes in Frage.

Der Deutsche Bundestag stellt fest, dass von Datenverarbeitungen in sozialen Netzwerken erhebliche Gefährdungen des Persönlichkeitsrechts ausgehen kön-

nen. Die Grundrechte auf informationelle Selbstbestimmung und auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sind nicht lediglich Abwehrrechte gegenüber staatlichen Stellen. Den Gesetzgeber treffen vielmehr umfängliche Schutzpflichten, um den Schutzgehalt dieser Grundrechte auch im nichtöffentlichen Bereich zu gewährleisten. Sowohl das deutsche als auch das europäische Datenschutzrecht weisen bislang nicht die erforderlichen, hinreichend präzisen gesetzlichen Bindungen für das Internetzeitalter, insbesondere für Betreiber sozialer Netzwerke auf. Die Datenschutzaufsichtsbehörden der Länder führen bereits seit einigen Jahren aufgrund der unterschiedlichsten Datenverarbeitungspraktiken aufwändige Konflikte mit einzelnen Anbietern sozialer Netzwerke, zuletzt vor allem mit Facebook, welche die deutschen Datenschutzbestimmungen für sich nicht für anwendbar halten. Die Datenschutzaufsichtsbehörden streben dabei regelmäßig und von vornherein weitgehende Kompromisse in Gestalt formloser Vereinbarungen an, weil Zweifel sowohl hinsichtlich der im Einzelnen anwendbaren Gesetze, als auch hinsichtlich des Anwendungsumfanges sowie der Möglichkeit der Durchsetzbarkeit von Anordnungen bestehen, die bei den meisten Anbietern auf Vollstreckungen im Ausland hinauslaufen würden. Bestehende Selbstverpflichtungsvereinbarungen einzelner Betreiber zugunsten besserer Datenschutzstandards werden derzeit von den Marktführern nicht mitgetragen und sind nicht, wie nach dem Bundesdatenschutzgesetz vorgesehen, mit den Aufsichtsbehörden abgestimmt. Der auch von der Bundesregierung noch immer favorisierte Weg der Selbstverpflichtung hat sich für einen effektiven Datenschutz der Nutzerinnen und Nutzer bislang auch in anderen Bereichen als wenig zielführend und nicht ausreichend erwiesen. Verstöße gegen Datenschutzbestimmungen können von den Verbraucherverbänden oft wegen fehlender Klagemöglichkeiten nicht effektiv bearbeitet werden.

Daneben ergeben sich auch Probleme werberechtlicher Art und des Jugendschutzes. Der Deutsche Bundestag sieht die Notwendigkeit, die bestehenden Jugendschutzbestimmungen an die neuen Anforderungen durch soziale Netzwerke anzupassen. Dies gilt insbesondere für Werbung, die sich an Kinder und Jugendliche richtet. Aufforderungen an Jugendliche, bestimmte nutzungsfördernde Handlungen vorzunehmen oder mehr Daten von sich preiszugeben, können unzulässig sein.

Werbliche Präsentationen müssen als solche deutlich erkennbar sein. Unlautere Gestaltungsmöglichkeiten („weghuschende Fenster“, „verdeckte Schließkreuze“ etc.) belästigen Nutzerinnen und Nutzer und erhöhen das Risiko ungewollter Vertragsabschlüsse.

II. Der Deutsche Bundestag fordert deshalb die Bundesregierung auf,

die allgemein mit dem Internet verbundenen, vielfältigen Rechtsunsicherheiten im Datenschutzrecht zu beseitigen, sich auf europäischer Ebene im Rahmen der angekündigten Reform des EG-Datenschutzrechts für eine umfassende Neuregelung mit dem Ziel der Verwirklichung eines hohen Schutzniveaus sowohl für den öffentlichen als auch den nichtöffentlichen Bereich einzusetzen und davon unabhängig bereits jetzt die bestehenden bundesdeutschen datenschutzrechtlichen Vorgaben zu präzisieren, insbesondere im Hinblick auf

1. die Anwendbarkeit und die Durchsetzbarkeit bundesdeutschen Datenschutzrechts gegenüber Unternehmen aus Drittstaaten außerhalb Europas. Leitlinie muss dabei die verbraucherfreundliche Geltendmachung der unterschiedlichen Datenschutzrechte für die betroffenen Nutzerinnen und Nutzer sowie die effektive Realisierung der Kontrollfunktion der Aufsichtsbehörden gegenüber denjenigen Anbietern sein, die sich mit ihren Angeboten gezielt an

bundesdeutsche Nutzerinnen und Nutzer und Verbraucherinnen und Verbraucher wenden. Im Hinblick auf eventuell entgegenstehende europäische Normen muss die Bundesregierung im Rahmen der anstehenden Reform der Datenschutzrichtlinie 95/46/EG parallel frühzeitig darauf hinwirken, dass über marktortbezogene Anknüpfungen nationale Schutzstandards gewährleistet werden und die einheitliche Behandlung unterschiedlicher Formen der Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Hinblick auf die Anwendbarkeit und Durchsetzbarkeit der Datenschutzbestimmungen unter Aufgabe der bislang erforderlichen territorialen Anknüpfung erfolgt;

2. die bessere Abgrenzung der sich teilweise überschneidenden Anwendungsbereiche des Telekommunikationsgesetzes, des Telemediengesetzes und des Bundesdatenschutzgesetzes. Im Rahmen einer umfassenderen Reform ist neben einer Vereinfachung und Vereinheitlichung der Rechtsbegriffe vor allem eine Zusammenführung der maßgeblichen Bestimmungen anzustreben;
3. das Recht der Nutzerinnen und Nutzer auf Löschung der von ihnen eingestellten Daten und das Recht Hinterbliebener auf die Löschung der Daten verstorbener Nutzerinnen und Nutzer;
4. die allgemeine, schon heute bestehende gesetzliche Verpflichtung der Anbieter von Telemediendiensten, pseudonyme bzw. anonyme Nutzungsmöglichkeiten anzubieten und Möglichkeiten des Selbstdatenschutzes wie etwa Anonymisierungsdienste zu fördern;
5. die Schaffung einer differenzierten, hinreichend flexiblen Verantwortlichkeitsregelung einschließlich entsprechender Haftungsregelungen für komplexe Datenverarbeitungen wie sie z. B. bei der Beteiligung mehrerer Stellen vorgenommen werden. Die Verteilung der Verantwortlichkeit sollte die jeweiligen tatsächlichen und wirtschaftlichen Einflussmöglichkeiten besonders berücksichtigen;
6. die Sicherstellung der Berücksichtigung von technischen Datenschutzlösungen, die bei neuen Systemen verpflichtend von Anfang an einzubauen sind (Grundsatz des Privacy by Design);
7. ein grundsätzliches Verbot der Profilbildung. Die Bildung von Profilen darf nur aufgrund spezieller gesetzlicher Grundlage oder durch (zeitlich begrenzte, jederzeit widerrufbare) informierte und ausdrückliche Einwilligungen möglich sein, die den spezifischen Risiken Rechnung tragen. Dies gilt insbesondere auch für die Hinzuziehung der Daten, die von anderen Anbietern in deren Internetpräsenzen integriert werden. Der Begriff der Profilbildung bedarf einer gesetzlichen Definition;
8. die Pflicht zur Bereitstellung von Diensten für neue Nutzer auf der Grundlage der jeweils strengsten Privatsphäre(grund)einstellungen (Grundsatz des Privacy by Default) bei gleichzeitiger Ermöglichung einer bedienfreundlichen und selektiven Freigabe von Informationen. Dabei ist für eine bedienerfreundliche Lösung bei Schutzeinstellungen Sorge zu tragen. Neue datenschutzrelevante, in die Dienste integrierte Angebote dürfen nicht standardmäßig durch den Anbieter aktiviert, sondern müssen vom Nutzer freigeschaltet werden;
9. die Ausweitung des Koppelungsverbots. Verträge dürfen nicht davon abhängig gemacht werden, dass die Betroffenen umfänglich in die Verarbeitung ihrer Daten u. a. zu Werbezwecken oder zur Profilbildung einwilligen;
10. die Verschärfung der Informationspflichten für Anbieter. Dazu zählt sowohl die Verpflichtung, die Nutzerinnen und Nutzer über alle Änderungen der Geschäfts- und Datenschutzbedingungen vorab in verständlicher Weise

und Sprache in Kenntnis zu setzen und zu dokumentieren, als auch die Pflicht, auf die konkreten Zwecke der Datenverarbeitung sowie auf die mit der Veröffentlichung personenbezogener Daten verbundenen Risiken hinzuweisen. Kinder und Jugendliche sind in einer altersangemessenen Sprache zu informieren;

11. die Pflicht, die automatisierte Erkennung biometrischer Merkmale wie z. B. Gesichtserkennungssoftware nur nach vorheriger informierter und vorab einzuholender ausdrücklicher Einwilligung einzusetzen. Die Ermöglichung der Veröffentlichung entsprechender Bilder setzt einen umfassenden Hinweis auch auf die mögliche Betroffenheit von Rechten Dritter voraus;
12. die Schaffung besonderer Schutzmaßnahmen bei Angeboten, die in besonderem Maße von Kindern und Jugendlichen genutzt werden, darunter ein vollständiges Verbot der Profilbildung für Jugendliche unter 16 Jahren;
13. das Verbot, die im Rahmen von Web-2.0-Angeboten erlangten Daten und Informationen dritter Personen, mit denen kein Vertragsverhältnis besteht, zu eigenen Zwecken zu erheben und zu verarbeiten;
14. die Schaffung offener Schnittstellen für die Ermöglichung des jederzeitigen Wechsels, das Recht auf Herausgabe der eigenen Daten und die Migration von persönlichen Kundendatenbeständen zwischen Anbietern;
15. die Schaffung eines allgemeinen Gütesiegel- und Auditierungsgesetzes, mit dessen Hilfe die unabhängige und auch vergleichende Bewertung von Produkten, Prozessen und Dienstleistungen auf ihre Datenschutzfreundlichkeit ermöglicht wird;
16. die Schaffung wirksamer Sanktionen für Datenschutzverstöße, wie eine Gefährdungshaftung auch für nichtöffentliche Stellen, eines pauschalisierten Schadensersatzes sowie die Erweiterung der Bußgeldtatbestände u. a. auf das unbefugte Nutzen von Daten und die Gefährdung durch Unterlassen der erforderlichen Schutzmaßnahmen;
17. die Schaffung eines ausdrücklichen Klageanspruches wegen der Verletzung datenschutzrechtlicher Regelungen im Unterlassungsklagegesetz, um durch Einbeziehung der Verbraucherschutzverbände die Kontrolldichte im Bereich der Privatwirtschaft zu erhöhen;
18. auf eine strenge Prüfung der Wirksamkeit der Bestimmungen des Safe-Harbor-Abkommens bei der Europäischen Kommission hinzuwirken und sich in Abhängigkeit des Ergebnisses der Prüfung ggf. für eine Aufhebung und Neuverhandlung einzusetzen. So sollten zukünftig auch Beschwerden der Aufsichtsbehörden eines europäischen Mitgliedstaates Verfahren seitens der Federal Trade Commission auslösen können;
19. auf die Verhandlungen über ein Datenaustauschabkommen mit den USA auf europäischer Ebene darauf zu drängen, dass ein allgemein hoher Schutzstandard für die Zulässigkeit der Übermittlung personenbezogener Daten festgelegt wird.

III. Der Deutsche Bundestag fordert ferner die Bundesregierung auf,

speziell in Bezug auf soziale Netzwerke Regelungen zu schaffen,

1. die im Rahmen einer gesonderten gesetzlichen Regelung zum Beschäftigtendatenschutz Bewerberrecherchen der Arbeitgeber grundsätzlich untersagen, soweit es sich um überwiegend zu privaten Zwecken genutzte soziale Netzwerke handelt;
2. mit denen im Hinblick auf mögliche Zugriffe sowohl von nationalen staatlichen Stellen als auch von Drittstaaten die Geltung des Grundrechts auf Ver-

traulichkeit und Integrität informationstechnischer Systeme, des Grundrechts auf Achtung des Kernbereichs der Persönlichkeit sowie des Grundrechts auf informationelle Selbstbestimmung effektiv sichergestellt wird;

3. die besondere Schutzvorkehrungen der Persönlichkeitsrechte Minderjähriger gewährleisten. Die Gestaltung von Werbung auf den Seiten sozialer Netzwerke, die von Kindern und Jugendlichen genutzt werden, ist so zu regulieren, dass unlautere Aufforderungen und Darstellungsformen untersagt werden;
4. die grundsätzlich die Auslesbarkeit von Profilen und nutzergenerierten Inhalten durch Suchmaschinen ausschließen;
5. um die Datensicherheit der von Nutzerinnen und Nutzern vorgehaltenen persönlichen Daten, insbesondere vor dem unbefugten Zugriff Dritter, effektiv sicherzustellen und dabei standardmäßig ein hohes Schutzniveau vorzugeben;
6. um die ständige und durch einfache Mechanismen unverzügliche Erreichbarkeit der Anbieter auch in Fragen des Datenschutzes sicherzustellen und insbesondere die jederzeitige, effektive, vollständige und rückstandslose Löschung der Daten der Nutzer sicherzustellen;
7. um auf die in Deutschland auftretenden Anbieter einzuwirken, gemeinsam mit Verbraucherschutzverbänden und den Datenschutzbeauftragten des Bundes und der Länder zusätzlich Selbstverpflichtungen einzugehen, die ggf. speziellere und einen hohen Standard des Schutzes persönlicher Daten und Informationen gewährleistende Regelungen zu weiteren Einzelfragen enthalten;
8. um in Abstimmung mit den Bundesländern ein Konzept zur Stärkung der Medienkompetenz vorzulegen, welches möglichst alle Altersklassen und Bildungsangebote erfasst und die Aufklärung über Chancen und Risiken sozialer Netzwerke, die damit einhergehenden Datenschutzrechte und die Möglichkeiten des Selbstschutzes der Nutzerinnen und Nutzer zum Ziel hat. Dabei sollten auch spezielle Informationen für Eltern und Lehrer einbezogen werden;
9. die sicherstellen, dass Userinnen und User Nutzungsrechte von selbst erstellten Inhalten nicht den Anbietern sozialer Netzwerke übereignen müssen.

Berlin, den 13. Dezember 2011

Renate Künast, Jürgen Trittin und Fraktion

Begründung

Soziale Netzwerke als besonders erfolgreiche Form von Netzgemeinschaften werden durch von privaten Unternehmen zur Verfügung gestellte technische Webanwendungen bzw. Portale betrieben.

Die Anzahl der Mitglieder sozialer Netzwerke steigt weiter rapide an. Insgesamt über 35 der 50 Millionen Bundesbürger im Internet sind in einem sozialen Netzwerk angemeldet. 77 Prozent der 13- bis 16-jährigen und 38 Prozent der neun- bis zwölfjährigen Internetnutzerinnen und -nutzer in der EU sind in Netzwerken aktiv. Die bekanntesten in Deutschland genutzten Dienste sind Facebook, Google+, die VZ-Netzwerke, myspace, Lokalisten, StayFriends, jappy,

wer kennt wen und XING. Allein 23 Millionen deutsche Nutzerinnen und Nutzer sind beim weltweiten Marktführer Facebook registriert, von denen mehr als 10 Prozent über ein vollständig offenes Profil verfügen, das selbst über einfache Google-Recherchen erschlossen werden kann.

Soziale Netzwerke sind inzwischen multifunktionale Plattformen. Jedes Netzwerk bietet den Nutzerinnen und Nutzern vor allem Möglichkeiten der Selbstpräsentation, Information über andere und Kommunikation mit anderen. Für jede dieser zentralen Funktionen bieten die Plattformen zumeist eine Vielzahl unterschiedlicher Instrumente.

Technisch bieten soziale Netzwerke die Möglichkeit der vollständigen Überwachung der Kommunikation und Nutzung des Internets. Die Datenskandale der vergangenen Jahre auch und gerade bei sozialen Netzwerken haben die besonderen Datenschutzrisiken für die Nutzerinnen und Nutzer des Internets verdeutlicht. Insbesondere die Datenschutzbeauftragten des Bundes und der Länder haben deshalb wiederholt Bemühungen des Gesetzgebers eingefordert, um die Internetfähigkeit der Datenschutzbestimmungen sowohl im Allgemeinen als auch für soziale Netzwerke im Besonderen herzustellen. Mit Ausnahme zweier thematisch begrenzter Reformen hat es jedoch in den vergangenen zehn Jahren keine entsprechende Modernisierung des Datenschutzes gegeben – mit der Konsequenz, dass die anzuwendenden Bestimmungen vielfach Auslegungsfragen aufwerfen und Rechtsstreitigkeiten nicht im Sinne des Rechtsfriedens beigelegt werden können, wie sich u. a. in den Fällen von Bewertungsportalen, bei den Geodatendiensten sowie zuletzt in der Auseinandersetzung der Datenschutzaufsichtsbehörden mit Facebook wegen der sogenannten Like Buttons und Fanpages gezeigt hat.

Der Präsident des Bundesverfassungsgerichts Prof. Dr. Andreas Voßkuhle erklärte kürzlich in einem dem Nachrichtenmagazin „FOCUS“ gegebenen Interview (6. November 2011), die Nutzung des Netzwerks Facebook sei eine gefahrengeneigte Tätigkeit, weil z. B. die Nutzer nicht wissen könnten, ob ihre Daten nach der Löschung nicht doch noch aufbewahrt würden. Er kritisierte die drohende Schieflage zwischen der Macht des Unternehmens und der auf 16 Bundesländer aufgeteilten Kontrolle der Datenschützer und deutete an, das Bundesverfassungsgericht könnte in den kommenden Jahren gezwungen sein, die Bedeutung und Reichweite der Grundrechte in einer Welt der digitalen Vernetzung neu zu bestimmen.

Die Bundesregierung hatte zunächst angekündigt, auf grundlegende Probleme des Persönlichkeitsschutzes des Internets mit einer Gesetzesinitiative antworten zu wollen. Ein Entwurf für das sogenannte Rote-Linie-Gesetz wurde jedoch bis heute nicht vorgelegt. Bereits im Koalitionsvertrag zwischen CDU, CSU und FDP hatte die Bundesregierung die Schaffung einer Stiftung Datenschutz angekündigt, deren Aufgaben allerdings unklar umrissen blieben und deren Gründung sich weiter verzögert. Zudem ist davon auszugehen, dass diese weder unabhängig noch in der Lage sein wird, eine Vergabe von Gütesiegeln eigenständig durchzuführen. Schließlich hatte die Bundesregierung auch eine zeitgemäße Überarbeitung der Bestimmungen des Bundesdatenschutzgesetzes auch zum Zwecke der besseren Verständlichkeit angekündigt. Anstelle der versprochenen Modernisierung legte sie den Entwurf eines Beschäftigtendatenschutzgesetzes vor, mit dem das kaum noch verständliche Bundesdatenschutzgesetz um weitere, systematisch kaum zu rechtfertigende und inhaltlich nahezu unleserliche Bestimmungen ergänzt werden soll. Es bestehen berechtigte Zweifel, ob der angesichts seiner erheblichen und offensichtlichen Mängel weitgehend unbrauchbare Gesetzentwurf tatsächlich Gesetz werden wird. Die Bilanz der Bundesregierung könnte somit darauf hinauslaufen, dass trotz des massiven Reformdruckes auch und gerade wegen der Entwicklungen des Internets keine

einzige gesetzliche Initiative zum Schutz der Daten und Informationen der Bürgerinnen und Bürger geschaffen wird.

Die von der EU-Kommission angekündigte Reform der Datenschutzrichtlinie 95/46/EG kann einen nationalen Reformprozess des Datenschutzrechts nicht ersetzen. Als übergreifende Regelung deckt sich das europäische Datenschutzrecht schon von seiner Funktion her nicht mit einer nationalen Regelung und lässt weitgehende Spielräume für bereichsspezifische Konkretisierungen. Auch der Ausgang des angekündigten EU-Reformvorhabens bleibt angesichts erwartbarer Widerstände sowohl in inhaltlicher als auch in zeitlicher Hinsicht weitgehend ungewiss.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333